



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/739,354	12/18/2003	Chad M. Fors	CE10577R/10-181	9648
22917	7590	01/22/2007	EXAMINER	
MOTOROLA, INC. 1303 EAST ALGONQUIN ROAD IL01/3RD SCHAUMBURG, IL 60196			YOUNG, NICOLE M	
			ART UNIT	PAPER NUMBER
			2112	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		01/22/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)
	10/739,354	FORS ET AL.
	Examiner Nicole M. Young	Art Unit 2112

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 12/18/2003.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-20 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 18 December 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>12/18/2003</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Drawings

The drawings are objected to because in Figs. 5 and 6, 515 and 615 should be labeled "Request Application Key" not "Retrieve Application Key."

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "429" has been used to designate both Store Application Keys and Derive Application Keys.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities:

Delete the second period after "concepts" on page 5, line 23.

On page 10 line 8, 304 should be added after 204, on line 9, 308 should be added after 208, and on line 17 "FIG. 1 and FIG. 2" should be "FIG. 2 and FIG. 3."

On page 12, "Key Manager 202" should be changed to read "Key Manager 203" on lines 8 and 11.

On page 20, line 8 the word registration is misspelled.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 11 and 13-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 11 is directed to a system entity. The specification (on page 13 paragraph 2) defines a system entity as a client or server that provides authentication services. On page 12 it states "specifically an application client." Therefore the system entity is interpreted as an application client composed entirely of software with no structural components. This is non-statutory subject matter under 35 U.S.C. 101. **Claims 13-20** are dependent claims on **claim 11** that do not further explain any structural components, therefore they are interpreted as software as well and are non-statutory.

Claim Rejections - 35 USC § 102

Art Unit: 2112

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9 and 11-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Zuk (US 5,745,571).

Claim 1:

Column 5 lines 1-26 teaches a smart card establishing contact with a point of sale and generating a random value r. This random value is used to create an “application, master or authentication key.” The key is later “used as a basis for generation of session keys for subsequent communication.” The Examiner interprets the “application, master or authentication key” as the dynamic seed and the “session key” as the application key.

Claim 2:

Column 5 lines 27-29 teach that the routines used to create the random key and session keys are erased “after the authentication key and other data has been stored.”

Claim 3:

Column 5 line 25 states “session keys.” The Examiner interprets this as multiple keys created for different applications.

Claim 4:

Column 5, lines 1-26 teach, "providing an application seed and generating key information specific to the application."

Claim 5:

The Examiner interprets that the session key of column 5 line 25 provides a new key every time the application needs to authenticate.

Claim 6:

The Examiner interprets that the session key of column 5 line 25 corresponds to a time duration that the communication of the client and server is valid.

Claim 7:

Column 4 and 5 describe the process of generating the dynamic seed and application keys. The Examiner interprets that this process is repeated for multiple dynamic seeds and application keys.

Claim 8:

Zuk discloses multiple smart cards authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Claim 9:

Column 2 lines 41-43 teach "a communications system comprising smart card means and a central processing station." The smart card is interpreted to be the client and the central processing station the network server.

Claim 11:

Art Unit: 2112

Column 5 lines 1-26 teaches a smart card establishing contact with a point of sale and generating a random value r. This random value is used to create an "application, master or authentication key." The key is later "used as a basis for generation of session keys for subsequent communication." The Examiner interprets the "application, master or authentication key" as the dynamic seed and the "session key" as the application key.

The Examiner interprets that this is implemented with a network access function as software. The key generation center (KGC) of these lines would be interpreted as the key manager.

Claim 12:

Column 5 lines 27-29 teach that the routines used to create the random key and session keys are erased "after the authentication key and other data has been stored."

Claim 13:

Column 5 line 25 states "session keys." The Examiner interprets this as multiple keys created for different applications.

Claim 14:

Column 5, lines 1-26 teach, "providing an application seed and generating key information specific to the application."

Claim 15:

The Examiner interprets that the session key of column 5 line 25 provides a new key every time the application needs to authenticate.

Claim 16:

The Examiner interprets that the session key of column 5 line 25 corresponds to a time duration that the communication of the client and server is valid.

Claim 17:

Column 4 and 5 describe the process of generating the dynamic seed and application keys. The Examiner interprets that this process is repeated for multiple dynamic seeds and application keys.

Claim 18:

Zuk discloses multiple smart cards, which include identity information, authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network, and it teaches Subscriber Identity Module extensions wherein the smart cards include authentication programming and identity information.

Claim 19:

Column 2 lines 41-43 teach "a communications system comprising smart card means and a central processing station." The smart card is interpreted to be the client and the central processing station the network server.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by **Pabla et al. (US 7,127,613)**.

Claim 1:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the

Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 2:

Column 6 lines 40-42 teach storing the session key for further use.

Claim 3:

Column 13 lines 1-14 teach creating groups and groups within groups with unique session keys. This is interpreted to be equivalent to a plurality of application keys where each application has a different key.

Claim 4:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 5:

Column 10 lines 22-28 teach using a key once per session and a new session key if the peers need to communicate again.

Claim 6:

It is interpreted by the Examiner that the session key corresponds to a time duration that the communication of the client and server is valid. This is further

discussed in column 3 lines 29-41 where it states, "the two peers may use the session key for as long as the current session lasts."

Claim 7:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Column 3 lines 29-41 disclose getting a new and different key when the pair needs to authenticate again.

Claim 8:

Pabla et al. discloses multiple peers authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Claim 9:

Column 2 line 57 teaches a client-server environment.

Claim 10:

Column 13 lines 32-34 teach wired and wireless networks.

Claim 11:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to

Art Unit: 2112

include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

The Examiner interprets that this method is implemented as software with a network access function and key manager.

Claim 12:

Column 6 lines 40-42 teach storing the session key for further use.

Claim 13:

Column 13 lines 1-14 teach creating groups and groups within groups with unique session keys. This is interpreted to be equivalent to a plurality of application keys where each application has a different key.

Claim 14:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 15:

Column 10 lines 22-28 teach using a key once per session and a new session key if the peers need to communicate again.

Art Unit: 2112

Claim 16:

It is interpreted by the Examiner that the session key corresponds to a time duration that the communication of the client and server is valid. This is further discussed in column 3 lines 29-41 where it states, "the two peers may use the session key for as long as the current session lasts."

Claim 17:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Column 3 lines 29-41 disclose getting a new and different key when the pair needs to authenticate again.

Claim 18:

Pabla et al. discloses multiple peers authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Column 7 lines 25-41 teach using the Transport Layer Security and the hardware listed in 42-53 is equivalent to a smart card.

Claim 19:

Column 2 line 57 teaches a client-server environment.

Claim 20:

Column 13 lines 32-34 teach wired and wireless networks.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

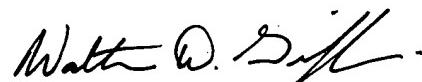
Buddhikot et al. discloses a system for authentication, dynamic key generation, session key authentication and wireless authentication. Brown et al. discloses a telecommunications network with session key authentication. Chen et al. discloses a shared secret key distribution system with session key authentication for online registration. Stanton et al. discloses a system and method of recovering the session key of an application for authentication purposes. Royer et al. discloses a system of communication protocols that authenticate applications through session keys.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-274-1382. The examiner can normally be reached on Monday through Friday, alt Friday off, 7:30-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY



**WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER**